REMARKS

Claims 1-3, 19, and 23-40 are pending in the present application. By this Amendment, claims 33-34 and 37-38 are amended to recite a computer program product comprising a computer-readable, tangible storage device and computer-readable program instructions stored on the computer-readable, tangible storage device to handle personally identifiable information. In addition, claims 27-32, and 39-40 are amended to recite a "computer" system and further to recite the computer elements of a CPU, a computer –readable memory, and a computer readable, tangible storage device, as well as program instructions, stored on the storage device for execution by the CPU via the memory. No new matter has been added by these amendments. Reconsideration of the claims is respectfully requested in view of the above amendments and the following remarks.

A. Rejection under 35 U.S.C. § 101

The Final Office Action rejects claims 33-38 under 35 U.S.C. § 101 as being allegedly directed to non-statutory subject matter. Specifically, the Final Office Action alleges that the medium recited in claims 33-38 may include carrier wave, signal, or transmission media.

By this Amendment, claim 33 is amended to recite a computer program product comprising a ***computer-readable, tangible storage device*** and computer-readable program instructions ***stored on the computer-readable, tangible storage device*** to handle personally identifiable information. Thus, the claims no longer recite a "computer readable storage medium" but rather a computer-readable, tangible storage device which is clearly directed to a statutory class of media, i.e. a device. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 33-38 under 35 U.S.C. § 101.

B. Rejection under 35 U.S.C. § 103(a) Based on King and Miller

1. Independent Claims 1, 27, and 33

The Final Office Action rejects claims 1-2, 23-24, 27, 29-30, 33, and 35-36 under 35

U.S.C. § 103(a) as being allegedly unpatentable over King (U.S. Patent No. 7,093,286) in view of Miller et al. (U.S. Patent Application Publication No. 2001/0054067). This rejection is respectfully traversed.

Claim 1, which is representative of the other rejected independent claims 27 and 33 with regard to similarly recited subject matter, reads as follows:

> 1. A method, in a data processing system, for handling personally identifiable information, said method comprising:
>
> providing, in a computer, ***a first set of object classes, of an object model in an object oriented programming language, representing active entities in an information-handling process***;
>
> providing, in said computer, ***a second object class, of the object model, representing personally identifiable information and associated rules in said information-handling process***; and
>
> processing transactions, in the data processing system, involving said personally identifiable information, using said computer and said ***first set of object classes and said second object class of the object model***, so as to enforce a privacy policy, wherein
>
> said rules define if and how ***said personally identifiable information is provided, by a first data user that previously requested the personally identifiable information from an active entity that is personally identifiable by the personally identifiable information, to a second data user that requests said personally identifiable information from the first data user.*** (emphasis added)

Applicants respectfully submit that neither King nor Miller, either alone or in combination, teaches or renders obvious at least those features of claim 1, and the similar features in the other rejected independent claims, emphasized above.

King is directed to a mechanism for communicating sensitive information in a wireless communication system. With the mechanism of King, the exchange, as well as the use and nature, of sensitive information released can be governed by one or more privacy agreements established between principle parties, namely a client device and a content server (column 5, lines 6-9). A proxy server device is used as a trusted third party such that, once a privacy agreement is established between the client and the content server, the content server can obtain sensitive information (which in the examples of King is location information) from either the client or the proxy server (column 5, lines 24-28). The sensitive information is provided from the client to the proxy server in requests sent by the client device or, alternatively, the proxy server can ask for the

information from the client device (column 6, lines 50-58).

The client may send a request to the proxy server which then forwards the request on to the content server. The content server may then request sensitive information from the proxy server. The proxy server then determines whether there is an existing privacy agreement between the client and the content server. If not, then the client and the content server must negotiate one prior to the exchange of the sensitive information (column 7, lines 20-35). A privacy manager on the proxy server may act as a negotiating agent between the client and the content server (column 9, lines 37-49).

Thus, with King, as long as a privacy agreement exists between a client and a server, then a third party entity, e.g., the proxy server, may provide sensitive information to the server on behalf of the client. If a privacy agreement does not exist between the client and the server, then one must be negotiated before the release of the sensitive information is allowed to happen.

It should first be noted that nowhere in King is there any mention of an object model being provided in an object oriented programming language. Furthermore, nowhere in King is there any teaching or technical rationale provided to implement such an object model that includes a first set of object classes representing active entities in an information-handling process, a second object class representing personally identifiable information and associated rules in the information handling process, or processing transactions using the first and second object classes in such an object model. King does mention "Handset Location Object (HLO)", "Network Location Object (NLO)", and an "Absolute Location Object (ALO)", but the term "object" in this context is being used generically to mean data; the term is not being used to refer to an object model in an object oriented programming language. However, even if the term "object" were being used to refer to objects in an object oriented programming language model, *arguendo*, at most these objects would represent sensitive information. There still would not be any mention of the particular objects set forth in claim 1, or the manner by which these objects in claim 1 are utilized to process transactions.

A key difference between King and the presently claimed invention as recited in claim 1 is that the privacy agreement in King is an agreement between the parties, i.e. the client and the content server, and is not tied to the particular sensitive information that is being communicated. That is, in the presently claimed invention, the rules, which specify if and how personally

identifiable information, about an active entity, may be provided by a first data user to a second data user, are tied to the actual personally identifiable information by being defined in a "second object class" of the object model, the second object class representing the ***personally identifiable information and associated rules***.

In King, the privacy agreement exists, or does not exist, independent of the sensitive information. This is clear in that King allows for the possibility that a server may request sensitive information from a proxy server and there may not be an existing privacy agreement to govern the transfer of such sensitive information and thus, one will be negotiated. Such a situation will not arise in the presently claimed invention since the personally identifiable information is tied to the rules governing its dissemination, by defining both the personally identifiable information and its associated rules in the second object class. Such a capability is not provided in the mechanism of King. In fact, as noted above, King does not even teach or provide any technical rationale to implement object classes of an object model in an object oriented programming language and thus, cannot teach such an object class representing the personally identifiable information and its associated rules.

Since King does not teach or render obvious object classes of an object model in an object oriented programming language, let alone the specific object classes recited in claim 1, King cannot teach or provide any technical rationale to process transactions using such object classes. To the contrary, King only looks to see if a privacy agreement exists between the client and the content server and if one does exist, then the sensitive information is allowed to be transmitted to the content server. King does not use a first set of object classes representing active entities in an information handling process, and a second object class representing personally identifiable information and its associated rules, to process transactions.

Moreover, the privacy agreement between the client and the content server in King does not define if and how the proxy server is able to provide the sensitive data, requested by the proxy server, to the content server that requested the sensitive data from the proxy server. To the contrary, the agreement between the client and the content server is merely an agreement that states that the content server is permitted to receive sensitive information about the client. It is not specifically directed to if and how the proxy server provides such information to the content server. Thus, the privacy agreement in King is not equivalent to the rules that define if and how ***said personally***

identifiable information is provided, by a first data user that previously requested the personally identifiable information from an active entity that is personally identifiable by the personally identifiable information, to a second data user that requests said personally identifiable information from the first data user.

The Miller reference, likewise, does not teach or render obvious the features of the claims missing from the teachings of King noted above. Miller is directed to a mechanism for driving navigation to a particular web site by detecting a docketing of a user's client device with a computer and opening a web page that is pre-designated to be opened upon docking of the client device with the computer.

Miller does not teach or provide any technical rationale to implement the features of providing, in a computer, ***a first set of object classes, of an object model in an object oriented programming language, representing active entities in an information-handling process***; providing, in said computer, ***a second object class, of the object model, representing personally identifiable information and associated rules in said information-handling process***; and processing transactions, in the data processing system, involving said personally identifiable information, using said computer and said ***first set of object classes and said second object class of the object model***, so as to enforce a privacy policy. Moreover, Miller does not teach or provide any technical rationale to implement the features that the rules define if and how ***said personally identifiable information is provided, by a first data user that previously requested the personally identifiable information from an active entity that is personally identifiable by the personally identifiable information, to a second data user that requests said personally identifiable information from the first data user.***

In fact, the Final Office Action does not cite Miller for teaching any of these features. To the contrary, the Miller reference is only cited for allegedly teaching the general concept of an object model in an object oriented programming language. However, the Final Office Action only states that Miller teaches collecting personally identifiable information and that the system of Miller is executed on a computer using JAVA or any object oriented programming at paragraphs [0043, 0125, and 0247] (see Final Office Action, page 8).

Paragraph [0043] is merely a generic paragraph describing a wide varieties of technologies that may be used to implement the mechanisms of the Miller reference, including

software based technologies. Paragraph [0125] describes that the Miller reference may collect personally identifiable information in order to provide services. Paragraph [0247] describes that the system of Miller may be implemented using JAVA or other object oriented programming mechanisms.

While Miller may teach object oriented programming may be used to implement a system for opening a web page upon docking a client computer, there is no teaching or technical rationale to apply these teachings to the mechanisms of King, let alone teaching or providing any technical rationale to implement the specific features of claim 1 that are missing from King as noted above, or the similar features of claims 27 and 33. Thus, since neither King nor Miller alone teach or provide any technical rationale to implement these features, any alleged combination of King and Miller would not result in these features being taught or rendered obvious. Therefore, contrary to the allegations raised in the Final Office Action, the alleged combination of King and Miller does not teach or render obvious the features of independent claims 1, 27, and 33.

Moreover, one of ordinary skill in the art would not have found it obvious to combine the teachings of King and Miller. King is directed to a mechanism for exchanging sensitive information in a wireless communication system and Miller is concerned with opening a web page when a client device is docked with a computer system. They are not related in any way and one of ordinary skill in the art would not have contemplated, let alone attempted to combine the teachings of Miller with King. One would not look to a system for opening a web page upon docking a client device for a solution to a problem associated with a mechanism for exchanging sensitive information in a wireless communication system, or vice versa. There simply is no correlation between the King and Miller references. However, even if one were somehow motivated to attempt the combination of King and Miller, the result still would not be the invention as recited in claims 1, 27, and 33, as discussed above.

2. Rebuttal of Examiner's Arguments

In response to the above arguments, the Examiner, in the Final Office Action alleges that King teaches in column 3, lines 37-38 that a computer program code for negotiating a privacy

agreement that governs the exchange of private information is described in King and that later in column 11, line 36 a sample of an accepted privacy agreement which includes a limitation of which information may be transmitted. The Final Office Action further states to see column 12, lines 22-24 (see Final Office Action, page 3, items 9-10).

These sections of King only teach what Applicants have stated above that King teaches, i.e. the negotiation of a privacy agreement that is a generic privacy agreement between the parties. Even if King teaches a privacy agreement, King still does not teach the specific features of the independent claims discussed above. The privacy agreement is still separate and distinct from the personally identifiable information and is generic to the relationship between the parties. It is not tied to the particular personally identifiable information in the manner of the presently claimed invention, as discussed above. Merely pointing to a section of the King reference that teaches that a privacy agreement governs the exchange of private information still does not teach the specific features of claim 1 discussed above, i.e. providing, in a computer, ***a first set of object classes, of an object model in an object oriented programming language, representing active entities in an information-handling process***; providing, in said computer, ***a second object class, of the object model, representing personally identifiable information and associated rules in said information-handling process***; processing transactions, in the data processing system, involving said personally identifiable information, using said computer and said ***first set of object classes and said second object class of the object model***, so as to enforce a privacy policy; and said rules define if and how ***said personally identifiable information is provided, by a first data user that previously requested the personally identifiable information from an active entity that is personally identifiable by the personally identifiable information, to a second data user that requests said personally identifiable information from the first data user***.

The Final Office Action further responds to the argument that King does not teach rules that define if and how said personally identifiable information is provided, by a first data user that previously requested the personally identifiable information from an active entity that is personally identifiable by the personally identifiable information, to a second data user that requests said personally identifiable information from the first data user, by pointing to column 9, lines 37-45 and column 14, lines 35-37 (see Final Office Action, page 4, items 11-12). As

reproduced in the Final Office Action, these sections of King mention that the privacy manager may generate user interfaces for the participants which define the information covered by the agreement, the term of the agreement, and how that information may be used. These sections further teach that a standing agreement pre-establishes terms and conditions for the release of location and related information and that the privacy agreement is a proposed agreement in which the content server specifies how private data is to be used by the content server.

Column 9, lines 37-45 and column 14, lines 35-37 of King are directed to the establishment of a privacy policy between two participants where the privacy policy only governs how one of the participants can use the information, i.e. the content server. Thus, when King says that the privacy agreement defines the information covered and how that information may be used, King is referred to how one of the parties can itself use the information, specifically how the server itself can use the private information supplied by the other party, e.g., the handset user.

To the contrary, the presently claimed invention recites that the rules define if and how said personally identifiable information is provided, ***by a first data user that previously requested the personally identifiable information from an active entity that is personally identifiable by the personally identifiable information, to a second data user that requests said personally identifiable information from the first data user***. Thus, the rules govern the dissemination of personally identifiable information among three parties in the presently claimed invention, i.e. the active entity, a first data user, and a second data user. The personally identifiable information is provided by the active entity to the first data user. The second data user requests the information from the first data user. The rules govern if and how this first data user can provide the information to the second data user. To the contrary, in King, the privacy policy only governs how the server can use information provided by the other party.

Thus, again, the King reference, taken alone or in combination with the Miller reference, does not in fact teach or render obvious the specific features of independent claims 1, 27 and 33. At least by virtue of their dependency on claims 1, 27, and 33, respectively, the alleged combination of King and Miller does not teach or render obvious the features of dependent claims 2, 23-24, 29-30, and 35-36. Accordingly Applicants respectfully request that the rejection of claims 1-2, 23-24, 27, 29-30, 33, and 35-36 under 35 U.S.C. § 103(a) be withdrawn.

3. Dependent Claims 2, 23-24, 29-30, and 35-36

a. Claim 2

In addition to the above, King does not teach the specific features of dependent claims 2, 23-24, 29-30, and 35-36. With regard to claim 2, King and Miller fail to teach or render obvious the feature that a first set of object classes includes one or more object classes representing parties, selected from the group consisting of: a data user object class, a data subject object class, a guardian object class, and a privacy authority object class. The Final Office Action alleges that this feature is taught by King at column 3, lines 15-16; column 4, lines 9-11; and in Figure 1, element 120 (see Final Office Action, page 8, item 24). Applicants respectfully disagree.

Column 3, lines 15-16 of King teaches "as a system for controlling information exchange between a wireless client device and server devices, the..." There is no mention of objects anywhere in this section, or any other section, of King, let along the particular object classes recited in claim 2. Column 4, lines 9-11 states "another advantage of the invention is that client devices (subscribers) of networks can control the release of their information with respect to server devices on the networks." Again, there is not one mention of objects, object classes, or any of the other features of claim 2. Element 120 in Figure 1 is a network server. Again, merely showing a network server does not provide any teaching or technical rationale to implement the feature of a first set of object classes includes one or more object classes representing parties, selected from the group consisting of: a data user object class, a data subject object class, a guardian object class, and a privacy authority object class.

Thus, King does not in fact teach or render obvious the features of claim 2. Miller, likewise, does not teach or render obvious these features and is not cited for teaching or rendering these features obvious. While Miller may generally teach the use of an object oriented programming language, Miller does not provide any teaching or technical rationale to implement the specific object classes or other features referencing these object classes recited in claim 2. Therefore, any alleged combination of King and Miller would still not result in these features being taught or rendered obvious. Accordingly, Applicants respectfully request that the rejection of claim 2 under 35 U.S.C. § 103(a) be withdrawn.

b. Claims 23, 29, and 35

With regard to claims 23, 29 and 35, King and Miller fail to teach or render obvious the features of a privacy policy being associated with the personally identifiable information and defined by the rules, and being enforced against one or more active entities represented by the first set of object classes, and wherein each of the one or more active entities represented by the first set of object classes is a human being or legal entity. As mentioned above, King does not even mention object classes of an object model, let alone any one of these specific object classes set forth in these claims or the use of such object classes.

The Final Office Action alleges that the features of these claims are taught by King at column 3, lines 15-30; column 5, lines 45-49; column 6, lines 50-65; column 7, lines 24-27; column 11, lines 40-41; and in the Abstract (see Final Office Action, page 9, item 25). Column 3, lines 15-30 of King discusses controlling information exchange between a wireless client device and server devices, but makes no mention of object classes, let alone the specific object classes recited in claims 23, 29, and 35. Column 5, lines 45-49 merely teaches that location information will not be released to a server unless a privacy agreement is in place between the wireless client device and the server. Column 6, lines 50-65 teaches that location information can be provided with requests from the client device or may be requested from the client device by a proxy server which then provides the location information to the server. Column 7, lines 24-27 merely teaches that the server can request location and other private information from the client device. Column 11, lines 40-41 merely teaches a component of a privacy agreement may include a text field used to describe the legal entity providing the service and entering into the agreement with the user agent. The Abstract merely gives a general overview that the mechanism of King is directed to the exchange of sensitive information between client devices and server devices by using privacy agreements between the client device and the content server and that a proxy server can be used to establish privacy agreements with content servers.

While all of these sections have relevance to the generally idea of the exchange of sensitive information between a client device and a content server, none of these sections teach or render obvious the specific features of a privacy policy being associated with the personally

identifiable information and defined by the rules, and being enforced against one or more active entities represented by the first set of object classes, and wherein each of the one or more active entities represented by the first set of object classes is a human being or legal entity. Again, as argued above, the privacy agreement in King is separate and distinct from the actual sensitive information and is not tied to it in any way. That is, in King, the privacy agreement may state that the client can send location information to the content server. The privacy agreement is a generic agreement and is not tied to any specific location information.

To the contrary, with the mechanisms of the illustrative embodiments, the privacy policy is associated with the particular personally identifiable information by being defined in the rules of the "second object class" which represents both the personally identifiable information and associated rules. King has not contemplation of any such object classes and in fact, as discussed repeatedly above, makes no mention of objects or object classes at all. While Miller mentions object oriented programming languages, Miller makes no mention and provides no technical rationale to implement the specific objects and object classes recited in the claim.

Thus, King does not in fact teach or render obvious the features of claims 23, 29, and 35. Miller, likewise, does not teach or render obvious these features and is not cited for teaching or rendering these features obvious. Therefore, any alleged combination of King and Miller would still not result in these features being taught or rendered obvious. Accordingly, Applicants respectfully request that the rejection of claims 23, 29, and 35 under 35 U.S.C. § 103(a) be withdrawn.

c. Claims 24, 30, and 36

Regarding claims 24, 30 and 36, King and Miller fail to teach or render obvious the features of a first active entity ***represented by a first object class in said first set of object classes*** being said ***first data user*** that previously requested said personally identifiable information from ***said data subject that is a second active entity represented by a second object class in said first set of object classes***, and ***a third active entity represented by a third object class in said first set of object classes*** being said ***second data user*** that requests said personally identifiable information from said first data user. Again, King does not teach any object classes at all, let

alone the specific object classes recited in the claims. Nowhere in King is there any teaching to represent the client, the proxy server, and the content server as objects in a first set of object classes that represent active entities. Nowhere in King is there any teaching to use such object classes, along with another object class representing the sensitive information and its associated rules, to process transactions. King only teaches to establish a privacy agreement between the client and the content server, and to have the proxy server ensure that such an agreement is in place before transmitting the sensitive information; otherwise an agreement must be negotiated before transmitting the sensitive information. King does not teach or provide any technical rationale to implement the specific features of claims 24, 30, and 36.

The Final Office Action points to the same sections of King discussed above with regard to the other dependent claims. As discussed above, these sections are relevant to the general concept of controlling the transfer of sensitive information from a client device to a content server, but other than that have no relevance to the particular features recited in the claims. None of these cited sections of King, or any other sections of King, teach or render obvious the specific features of claims 24, 30, and 36 noted above. Moreover, as repeatedly stated above, Miller is only cited for teaching an object oriented programming language and does not provide any teaching or technical rationale to implement the features of the claims that are missing from the King reference.

Thus, King does not in fact teach or render obvious the features of claims 24, 30, and 36. Miller, likewise, does not teach or render obvious these features and is not cited for teaching or rendering these features obvious. Therefore, any alleged combination of King and Miller would still not result in these features being taught or rendered obvious. Accordingly, Applicants respectfully request that the rejection of claims 24, 30, and 36 under 35 U.S.C. § 103(a) be withdrawn.

C. Rejection under 35 U.S.C. § 103(a) Based on King, Miller and Tolopka

The Final Office Action rejects claim 3 under 35 U.S.C. § 103(a) as being allegedly unpatentable over King (U.S. Patent No. 7,093,286) in view of Miller, and further in view of Tolopka (U.S. Patent No. 6,044,349). This rejection is respectfully traversed for at least the same

reasons as set forth above with regard to the 35 U.S.C. § 102(e) rejection based on King and Miller. That is, King and Miller fail to teach or render obvious the features discussed above in independent claim 1, from which claim 3 depends. Moreover, Tolopka does not provide any teaching or technical rationale to implement the features missing from King and Miller as noted above.

Claim 3 reads as follows:

> 3. The method of claim 1, wherein said second object class, having said rules associated with said data, ***represents a filled paper form, including both collected data, collected from the active entity and including the personally identifiable information, and rules regarding said collected data specifying if and how the collected data is provided to the second data user***, wherein ***the second data user sends an empty form including a policy to the first data user requesting the personally identifiable information***, and wherein ***the first data user checks the policy included with the empty form to determine if disclosure of the personally identifiable information is permitted based on the policy included with the empty form and the rules regarding the collected data.***
> (emphasis added)

Neither King, Miller, nor Tolopka, either alone or in combination, teach or render obvious at least those features of claim 3 emphasized above.

Tolopka is directed to a portable storage medium to store data and provide access to information from an information dissemination system (IDS). The storage medium can store one or more location/key pairs. Each of the location/key pairs designates a particular IDS location as well as an access key to the particular IDS location. The storage medium can also store a plurality of information units. The information units are categorized into levels of information categories with at least one information category per level and at least one information unit per information category. Levels of information categories can be individually accessed and categories of information units within levels can be selectively downloaded.

Thus, Tolopka is only concerned with what access a particular information seeking system has to an IDS, and controls this acess based on a key provided on a smart card. The key and smart card in Tolopka operate in a similar manner as Access Control Lists (ACLs) in that they only control access by that particular subject, or information seeking system, to a particular object. They do not have anything to do with controlling how the information seeking system

may then send that information to another information seeking system. Moreover, the key and smart card mechanism of Tolopka does not provide any teaching, or even suggestion, regarding a filled paper form, including both collected data, collected from the active entity and including the personally identifiable information, and rules regarding said collected data specifying if and how the collected data is provided to the second data user. Tolopka at most teaches adding labels and data to a table.

The Final Office Action points to column 6, lines 36-52 of Tolopka as allegedly teaching objects that may represent paper-filled forms. Applicants respectfully submit that this section of Tolopka states that the user may manually type information with a text editor or other application and download it to the storage medium such that user entered labels, and apparently the data, may be added to the table shown in Figure 2, which is a depiction of information categories and information units stored on the storage medium (see Tolopka, Brief Description of the Drawings). Simply because the user can add labels and data to a data structure, which is depicted as a table in Figure 2, does not mean that Tolopka teaches an object class having rules associated with data that represents a filled paper form including both collected data and rules regarding the collected data, as recited in claim 3. The table in Figure 2 of Tolopka is not an object class representing a filled paper form and furthermore, does not include both collected data and rules regarding the collected data.

Furthermore Tolopka fails to teach or render obvious the features of the second data user sending an empty form including a policy to the first data user requesting the personally identifiable information, and wherein the first data user checks the policy included with the empty form to determine if disclosure of the personally identifiable information is permitted based on the policy included with the empty form and the rules regarding the collected data. To the contrary, Tolopka merely teaches that a user may edit a data structure and store it on a storage medium. Neither Tolopka, King, nor Miller, either alone or in combination, teach or render obvious such exchange of forms and checking of policies with rules as set forth in claim 3.

1. Rebuttal of Examiner's Argument

In response to these arguments, the Examiner, in the Final Office Action, states that the

combination of references include the teaching of King regarding negotiating a privacy agreement, the teaching of Miller of objects in an object class of an object oriented language, and the teaching of Tolopka that information may represent a paper filled form (see Final Office Action, pages 4-5, items 14-15). Applicants respectfully submit that Tolopka does not teach that information may represent a paper filled form as discussed above. Applicants respectfully submit that while Miller may generally teach object oriented programming languages, Miller makes no teaching and provides no technical rationale to implement the specific objects and object classes of an object model specifically recited in the present claims. Furthermore, Applicants respectfully submit that King only teaches a privacy agreement between a client and a content server regarding the information that the client can provide to the content server and the use that the content server can make of the information provided by the client. The privacy agreement in King does not govern if and how the content server can provide the information to other requesters of the information that contact the content server for the information. Thus, the Examiner's rebuttal does not address the specific arguments presented and merely rehashes the Examiner's position set forth in the rejection of the claims.

In view of the above, Applicants respectfully submit that the alleged combination of King, Miller and Tolopka does not teach or render obvious the features of claim 3. Accordingly, Applicants respectfully request that the rejection of claim 3 under 35 U.S.C. § 103(a) be withdrawn.

D. Rejection under 35 U.S.C. § 103(a) Based on King, Miller and Gifford

The Final Office Action rejects claims 19, 25-26, 28, 31-32, 34, and 37-38 under 35 U.S.C. § 103(a) as being allegedly unpatentable over King in view of Miller, and further in view of Gifford (U.S. Patent No. 5,614,927). This rejection is respectfully traversed for at least the same reasons as set forth above with regard to the 35 U.S.C. § 102(e) rejection based on King and Miller. That is, King and Miller fail to teach or render obvious the features discussed above with regard to independent claims 1, 27, and 33 from which claims 19, 25-26, 28, 31-32, 34, and 37-38 depend, respectively. Moreover, Gifford does not provide any teaching or technical rationale to implement the features of the independent claims that are missing from King and

Miller as noted above.

1. Claims 19, 28, and 34

Gifford is directed to a system and method for protecting a database against deduction of confidential attribute values therein. A memory is provided for storing the database and a processor is provided for processing the database. Using the processor, the database is electronically partitioned into public attributes, containing non-confidential attribute values, and private attributes, containing private attribute values. The processor is then used to electronically process the private attribute values to reduce any high correlation between public attribute values and private attribute values.

Gifford is cited by the Final Office Action as allegedly teaching depersonalization of objects at column 8, lines 1-8. Column 8, lines 1-8 teaches that after partitioning a database, the correlation between public attributes and private attributes is reduced by camouflaging some highly correlative public attribute values and outright removing some tuples containing highly correlative public attribute values which are difficult to camouflage.

With regard to claims 19, 28, and 34, neither King, Miller, nor Gifford, either alone or in combination, teach or render obvious the features of transforming, based on said rules, said personally identifiable information into a depersonalized format prior to providing said personally identifiable information to the second data user. Camouflaging the correlation between a public attribute and a private attribute in a partitioned database does not teach or render obvious the specific features of transforming, based on rules, personally identifiable information into a ***depersonalized format prior to providing the personally identifiable information to the second data user***. All that Gifford teaches is that the link between one attribute and another is camouflaged within a database. Breaking the link between attributes within a database does not cause personally identifiable information that is being sent to a second data user to be depersonalized prior to the sending of that information to second data user. To the contrary, it merely prevents someone from accessing the database to obtain private attributes by following the link from a public attribute to the private attribute. Furthermore, King and

Miller do not teach or provide any technical rationale to depersonalize information being provided to the content server, as recognized by the Final Office Action (Final Office Action, page 11, item 30). Thus, contrary to the allegations in the Final Office Action, Gifford does not in fact teach or render obvious the features of claims 19, 28, and 34, whether taken alone or in combination with King and Miller.

2. Rebuttal of Examiner's Argument

In response to this argument, the Examiner states that the rejection is based on the teaching of Gifford reference regarding protecting confidential information in a database. This is basically just restating the position the Examiner takes in the actual rejection that somehow a general teaching of protecting information in a database by breaking the link between one attribute and another in the database somehow teaches the specific features of transforming, based on rules, personally identifiable information into a ***depersonalized format prior to providing the personally identifiable information to the second data user***. There is not even a mention of providing the content of the database to a second data user or performing the "camouflaging" of the confidential information by breaking the links between the attributes prior to providing the database to a second data user. There simply is no teaching or technical rationale provided in Gifford to implement the specific features of the claim. Moreover, there is no teaching or technical rationale in King or Miller regarding any need or desire to incorporate a mechanism for breaking links between attributes of a database, such as taught in Gifford.

Thus, contrary to the allegations raised in the Final Office Action, the alleged combination of King, Miller, and Gifford does not in fact teach or render obvious the specific features of claims 19, 28, and 34. Accordingly, Applicants respectfully request that the rejection of claims 19, 28, and 34 under 35 U.S.C. § 103(a) be withdrawn.

3. Claims 25, 31 and 37

With regard to claims 25, 31, and 37, neither King, Miller nor Gifford, either alone or in combination, teach or render obvious the features of the transforming, based on the rules, of the

personally identifiable information into a depersonalized format prior to providing the personally identifiable information to the second data user comprises ***removing information that relates the personally identifiable information to the data subject in a reversible manner***. Again, merely severing the link between public attributes and private attributes in a database, as taught by Gifford, does not cause information to be removed from personally identifiable information that relates the personally identifiable information to a data subject ***in a reversible manner*** prior to the personally identifiable information being provided to a second data user.

Furthermore, as noted above, the Final Office Action admits that King and Miller do not teach such features either. Thus, any alleged combination of King, Miller and Gifford still would not teach or render such features obvious. To the contrary, the combination of King, Miller and Gifford would be some concoction primarily as presented by King in which some database somewhere that has private and public attributes has the links between private and public attributes severed as taught by Gifford. It is not at all clear how the general teaching of object oriented programming languages as taught by Miller would be specifically incorporated. The result of the alleged combination, assuming such a combination were possible and one were somehow motivated to combine the teachings of the references, *arguendo*, would not be the invention as recited in claims 25, 31, and 37.

4. Rebuttal of Examiner's Argument

In response to this argument, the Examiner again just reiterates the position set forth in the rejection of these claims (see Final Office Action, page 5, items 16-17). Simply reiterating the same position when Applicants have shown the error in such a position does not provide any reasoned explanation as to how Applicants are allegedly incorrect. Thus, it is believed that Applicants position as set forth above with regard to the features of claims 25, 31, and 37 is correct and is compelling.

Thus, contrary to the allegations raised in the Final Office Action, the alleged combination of King, Miller, and Gifford does not in fact teach or render obvious the specific features of claims 25, 31, and 37. Accordingly, Applicants respectfully request that the rejection of claims 25, 31, and 37 under 35 U.S.C. § 103(a) be withdrawn.

5. Claims 26, 32, and 38

Regarding claims 26, 32, and 38, neither King, Miller nor Gifford, either alone or in combination, teach or render obvious the features of the transforming, based on the rules, of the personally identifiable information into an anonymized format prior to providing said personally identifiable information to the second data user, ***wherein the anonymized format is a format in which all elements that may allow the personally identifiable information to be related to the data subject are stripped off in a non-reversible manner***. Again, Gifford only teaches severing the link between public and private attributes within a database such that one cannot use a public attribute to gain access to the private attribute. Gifford does not teach or provide any technical rational to depersonalize personally identifiable information that is to be provided to a second data user prior to the information being provided to the second data user by stripping off all elements that may allow the personally identifiable information to be related to the data subject.

Furthermore, as noted above, the Final Office Action admits that King and Miller do not teach such features either. Thus, any alleged combination of King, Miller and Gifford still would not teach or render such features obvious. The result of the alleged combination, assuming such a combination were possible and one were somehow motivated to combine the teachings of the references, *arguendo*, would not be the invention as recited in claims 26, 32, and 38.

6. Rebuttal of Examiner's Argument

In response to this argument, the Examiner again just reiterates the position set forth in the rejection of these claims (see Final Office Action, page 5, items 16-17). Simply reiterating the same position when Applicants have shown the error in such a position does not provide any reasoned explanation as to how Applicants are allegedly incorrect. Thus, it is believed that Applicants position as set forth above with regard to the features of claims 26, 32, and 38 is correct and is compelling.

Thus, contrary to the allegations raised in the Final Office Action, the alleged combination of King, Miller, and Gifford does not in fact teach or render obvious the specific

features of claims 26, 32, and 38. Accordingly, Applicants respectfully request that the rejection of claims 26, 32, and 38 under 35 U.S.C. § 103(a) be withdrawn.

E. Conclusion

It is respectfully urged that the subject application is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,

Date: October 12, 2010

Stephen J. Walder, Jr.
Registration No. 41,534
WALDER INTELLECTUAL PROPERTY LAW, P.C.
17330 Preston Road, Suite 100B
Dallas, Texas 75252
(972) 380-9475
ATTORNEY FOR APPLICANTS